คู่มือการปฏิบัติงาน
การตรวจ IT Security & Cyber Security
(IT General Control)
สำหรับนักวิชาการตรวจสอบภายใน

กลุ่มตรวจสอบภายใน สำนักงานบริหารหนี้สาธารณะ กระทรวงการคลัง

คำนำ

คู่มือการปฏิบัติการตรวจ IT Security & Cyber Security (IT General Control) ของกลุ่มตรวจสอบภายใน สำนักงานบริหารหนี้สาธารณะ กระทรวงการคลัง จัดทำขึ้นโดยมีเนื้อหาครอบคลุมกระบวนการปฏิบัติงานตรวจติดตามข้อเสนอแนะของหน่วยรับตรวจ ซึ่งแสดงขั้นตอน วิธีการตรวจตั้งแต่เริ่มต้นจนสิ้นสุดกระบวนการตรวจสอบ

ผู้จัดทำหวังเป็นอย่างยิ่งว่าคู่มือดังกล่าวจะเกิดประโยชน์แก่ผู้ตรวจสอบภายใน ในการปฏิบัติงานด้านตรวจสอบภายในให้สามารถปฏิบัติงานบรรลุวัตถุประสงค์ของผู้ตรวจสอบภายใน รวมทั้งเพิ่มคุณค่าให้กับองค์กรมากยิ่งขึ้น

ผู้จัดทำ นายวรุณกานต์ พรมรัตน์
นักวิชาการตรวจสอบภายใน กลุ่มตรวจสอบภายใน
สำนักงานบริหารหนี้สาธารณะ กระทรวงการคลัง

สารบัญ

หน้า

คำนำ **ก**

สารบัญ **ข**

บทที่ ๑ ขั้นตอนการดำเนินงานและวิธีการในการตรวจสอบ

ประเด็นการตรวจสอบ ๑

วัตถุประสงค์การตรวจสอบ ๑

ขอบเขตการตรวจสอบ ๑

ประเด็น ขั้นตอน และวิธีการดำเนินงาน ๒

บทที่ ๒ เอกสารหลักฐานที่ใช้ในการตรวจสอบ

เอกสารสำคัญต่างๆ ๔

บทที่ ๓ ระเบียบที่เกี่ยวข้อง

ระเบียบที่เกี่ยวข้องต่างๆ ๕

ภาคผนวก

ตัวอย่างการประเมินความเสี่ยง IT Security & Cyber Security (IT General Control) ๗

ตัวอย่างกระดาษทำการ IT Security & Cyber Security (IT General Control) ๑๑

บทที่ ๑
ขั้นตอนการดำเนินงานและวิธีการ
ในการตรวจสอบ

เริ่มจากการนำ RISK BASED AUDIT (RBA) มาประเมินความเสี่ยง เพื่อการจัดทำแผนการตรวจสอบ กำหนดประเด็นการตรวจสอบ เพื่อกำหนดวัตถุประสงค์ของการตรวจสอบ
(เอกสารการประเมินความเสี่ยง ตารางที่ ๑ และตารางที่ ๒)
นำผลการประเมินความเสี่ยงที่ได้มาจัดทำแผนปฏิบัติงานตรวจสอบการดำเนินงานตรวจ IT Security & Cyber Security (IT General Control) โดยกำหนดประเด็นการตรวจสอบ วัตถุประสงค์ และขอบเขตการตรวจสอบ ดังนี้

ประเด็นการตรวจสอบ :

๑. การควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (General Control) มีประสิทธิภาพ ครอบคลุมการปฏิบัติงานด้านเทคโนโลยีสารสนเทศของ สบน.

๒. การดำเนินการตามระบบ IT Security

๓. การดำเนินการตามระบบ Cyber Security

วัตถุประสงค์การตรวจสอบ :

๑. เพื่อสอบทานการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (General Control)

๒. เพื่อสอบทานการดำเนินการตามระบบ IT Security ว่า มีความเหมาะสม เพียงพอ

๓. เพื่อสอบทานการดำเนินการตามระบบ และ Cyber Security ว่า มีความเหมาะสม เพียงพอ

ขอบเขตการตรวจสอบ :

๑. การสอบทานการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (General Control)

๑) นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคลของ สบน.

๒) โครงสร้างทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

๓) การควบคุมการเข้าถึง เช่น การควบคุมการเข้าถึงระบบสารสนเทศ การจัดการการเข้าถึงระบบของบุคลากร การควบคุมระบบและโปรแกรมประยุกต์ เป็นต้น

๔) ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อมขององค์กร เช่นบริเวณที่ต้องมีการรักษาความปลอดภัย และการป้องกันอุปกรณ์ต่างๆ ขององค์กร เป็นต้น

๕) ความปลอดภัยในการปฏิบัติงาน เช่น การกำหนดหน้าที่ความรับผิดชอบ และวิธีการปฏิบัติงานการป้องกันมัลแวร์ การติดตั้งโปรแกรมบนระบบปฏิบัติการ การบันทึก Log และการเฝ้าดู เป็นต้น

๖) การควบคุมการพัฒนา และการบำรุงรักษาระบบสารสนเทศ

๒. การสอบทานการดำเนินการตามระบบ IT Security

๑) การรักษาความปลอดภัยเครือข่าย (Network Security)

๒) การรักษาความปลอดภัยอินเทอร์เน็ต (Internet Security)

๓) การรักษความปลอดภัยอุปกรณ์ปลายทาง (Endpoint Security)

๔) การรักษาความปลอดภัยระบบคลาวด์ (Cloud Security)

๕) การรักษาความปลอดภัยการเข้าใช้งานแอปพลิเคชั่น (Application Security)

๓. การสอบทานการดำเนินการตามระบบ Cyber Security

๑) การรักษาความปลอดภัยของระบบโครงสร้างพื้นฐาน (Critical Infrastructure Security)

๒) การรักษาความปลอดภัยระบบแอปพลิเคชั่น (Application Security) เช่น โปรแกรม Antivirus, Firewall หรือโปรแกรมการเข้ารหัส เป็นต้น

๓) การรักษาความปลอดภัยของระบบอินเทอร์เน็ต (Network Security)

๔) การรักษาความปลอดภัยให้กับข้อมูลที่เก็บในคลาวด์ (Cloud Security)

๕) การรักษาความปลอดภัยให้กับอุปกรณ์ Internet of Thing (Internet of Thing Security)

ประเด็น ขั้นตอน และวิธีการดำเนินงาน :

ประเด็น	วิธีการดำเนินงาน
๑. การควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (General Control) มีประสิทธิภาพ ครอบคลุมการปฏิบัติงานด้านเทคโนโลยีสารสนเทศของ สบน.	การสอบทานการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (General Control) ๑) นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคลของ สบน. ๒) โครงสร้างทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ๓) การควบคุมการเข้าถึง เช่น การควบคุมการเข้าถึงระบบสารสนเทศ การจัดการการเข้าถึงระบบของบุคลากร การควบคุมระบบและโปรแกรมประยุกต์ เป็นต้น ๔) ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อมขององค์กร เช่นบริเวณที่ต้องมีการรักษาความปลอดภัยและการป้องกันอุปกรณ์ต่างๆ ขององค์กร เป็นต้น ๕) ความปลอดภัยในการปฏิบัติงาน เช่น การกำหนดหน้าที่ความรับผิดชอบ และวิธีการปฏิบัติงาน การป้องกันมัลแวร์ การติดตั้งโปรแกรมบนระบบปฏิบัติการ การบันทึก Log และการเฝ้าดู เป็นต้น ๖) การควบคุมการพัฒนา และการบำรุงรักษาระบบ
๒. การดำเนินการตามระบบ IT Security	การสอบทานการดำเนินการตามระบบ IT Security ๑) การรักษาความปลอดภัยเครือข่าย (Network Security) ๒) การรักษาความปลอดภัยอินเทอร์เน็ต (Internet Security) ๓) การรักษความปลอดภัยอุปกรณ์ปลายทาง (Endpoint Security) ๔) การรักษาความปลอดภัยระบบคลาวด์ (Cloud Security) ๕) การรักษาความปลอดภัยการเข้าใช้งานแอปพลิเคชั่น (Application Security)

ประเด็น	วิธีการดำเนินงาน
๓. การดำเนินการตามระบบ Cyber Security	การสอบทานการดำเนินการตามระบบ Cyber Security ๑) การรักษาความปลอดภัยของระบบโครงสร้างพื้นฐาน (Critical Infrastructure Security) ๒) การรักษาความปลอดภัยระบบแอปพลิเคชั่น (Application Security) เช่น โปรแกรม Antivirus, Firewall หรือโปรแกรมการเข้ารหัส เป็นต้น ๓) การรักษาความปลอดภัยของระบบอินเทอร์เน็ต (Network Security) ๔) การรักษาความปลอดภัยให้กับข้อมูลที่เก็บในคลาวด์ (Cloud Security) ๕) การรักษาความปลอดภัยให้อุปกรณ์ Internet of Thing (Internet of Thing Security)

บทที่ ๒
เอกสารหลักฐานที่ใช้ในการตรวจสอบ

เอกสารหลักฐานที่ใช้ในการตรวจสอบ

๑) นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคลของ สบน.

๒) ขั้นตอน/คู่มือการปฏิบัติงานที่มีการปรับปรุงให้เป็นปัจจุบัน

๓) การกำหนดผู้รับผิดชอบการดำเนินการด้านเทคโนโลยีสารสนเทศ

๔) การกำหนดสิทธิ การทบทวนสิทธิ และรหัสผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

๕) ตัวชี้วัดรายบุคคล (KPI) ประจำปีงบประมาณ พ.ศ. ๒๕๖๕

๖) เอกสาร และหลักฐานต่างๆ ที่เกี่ยวข้อง

บทที่ ๓
ระเบียบที่เกี่ยวข้อง

ระเบียบที่เกี่ยวข้อง

๑. พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๒. คณะกรรมการพัฒนาระบบข้อมูลสารสนเทศของ สบน. (คณะกรรมการฯ)

๓. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานบริหารหนี้สาธารณะ (สบน.)

๔. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๑) พ.ศ. ๒๕๕๓ และฉบับที่ ๒ พ.ศ. ๒๕๕๖

๕. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

๖. พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๑) พ.ศ. ๒๕๕๐ และฉบับที่ ๒ (พ.ศ. ๒๕๖๐)

ภาคผนวก

ตัวอย่างการประเมินความเสี่ยงการตรวจสอบ IT Security & Cyber Security
(IT General Control)

ความเสี่ยง	การควบคุมที่มีอยู่	กิจกรรมที่จะตรวจสอบ
๑. การควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (General Control) ไม่มีประสิทธิภาพเพียงพอ	๑. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานบริหารหนี้สาธารณะ (สบน.) ๒. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๑) พ.ศ. ๒๕๕๓ และฉบับที่ ๒ พ.ศ. ๒๕๕๖ ๓. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ ๔. พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๑) พ.ศ. ๒๕๕๐ และฉบับที่ ๒ (พ.ศ. ๒๕๖๐)	๑. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูล ส่วนบุคคลของ สบน. ๒. โครงสร้างทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ๓. การควบคุมการเข้าถึง เช่น การควบคุมการเข้าถึงระบบสารสนเทศ การจัดการการเข้าถึงระบบของบุคลากร การควบคุมระบบและโปรแกรมประยุกต์ เป็นต้น ๔. ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อมขององค์กร เช่น บริเวณที่ต้องมีการรักษาความปลอดภัย และการป้องกันอุปกรณ์ต่างๆ ขององค์กร เป็นต้น ๕. ความปลอดภัยในการปฏิบัติงาน เช่น การกำหนดหน้าที่ความรับผิดชอบ และวิธีการปฏิบัติงาน การป้องกัน มัลแวร์ การติดตั้งโปรแกรมบนระบบปฏิบัติการ การบันทึก Log และการเฝ้าดู เป็นต้น ๖. การควบคุมการพัฒนา และการบำรุงรักษาระบบสารสนเทศ
๒. IT Security ไม่มีประสิทธิภาพเพียงพอ	๑. คณะกรรมการพัฒนาระบบข้อมูลสารสนเทศของ สบน. (คณะกรรมการฯ) ๒. การปฏิบัติงานด้านการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอาจไม่ตรงกัน และ/หรือไม่สอดคล้องตามกลยุทธ์ หรือวิสัยทัศน์ของ สบน. ทำให้ไม่สามารถปฏิบัติงานด้านบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ ๓. มีการรักษาความปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security) ที่ครอบคลุมถึงการบริหารจัดการการเปลี่ยนแปลง การบริหารจัดการขีดความสามารถของระบบ การรักษาความปลอดภัย	๑. การรักษาความปลอดภัยเครือข่าย (Network Security) ๒. การรักษาความปลอดภัยอินเทอร์เน็ต (Internet Security) ๓. การรักษความปลอดภัยอุปกรณ์ปลายทาง (Endpoint Security) ๔. การรักษาความปลอดภัยระบบคลาวด์ (Cloud Security) ๕. การรักษาความปลอดภัยการเข้าใช้งานแอปพลิเคชั่น (Application Security)

ความเสี่ยง	การควบคุมที่มีอยู่	กิจกรรมที่จะตรวจสอบ
๒. IT Security ไม่มีประสิทธิภาพเพียงพอ (ต่อ)	ของเครื่องแม่ข่าย การจัดเก็บข้อมูลบันทึกเหตุการณ์และติดตามดูแลระบบและการเฝ้าระวังภัยคุกคาม ๔. มีการติดตามดูแลระบบและการเฝ้าระวังภัยคุกคาม (Security Monitoring)	
๓. Cyber Security : การป้องกันระบบเทคโนโลยีสารสนเทศจากภัยคุกคามทางไซเบอร์ เนื่องจากเป็นเทคโนโลยีเก่าและมีอายุการใช้งานนานกว่า ๕ ปี รวมถึงภัยคุกคามที่มีการพัฒนาและปรับเปลี่ยนรูปแบบตลอดเวลา	๑. พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ๒. คณะกรรมการพัฒนาระบบข้อมูลสารสนเทศของ สบน. (คณะกรรมการฯ) ๓. มีแนวปฏิบัติด้านการเข้ารหัสข้อมูล (Cryptography) ในการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสมตามชั้นความลับและความสำคัญของข้อมูลสารสนเทศ ๔. มีการรรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสารของบริษัท (Network and Communication Security) โดยมีการป้องกันข้อมูลที่มีการรับส่งผ่านเครือข่ายให้มีความปลอดภัย สามารถป้องกันและเฝ้าระวังการถูกบุกรุกหรือภัยคุกคามที่อาจเกิดขึ้นได้ ๕. มีการจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging) ของเครื่องแม่ข่ายระบบงานและอุปกรณ์เครือข่ายที่สำคัญ โดยจะต้องมีความมั่นคงปลอดภัยเพียงพอในการป้องกันการเปลี่ยนแปลง แก้ไขหรือทำลาย รวมถึงมีการสอบทาน log ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ๖. ปรับปรุงสถาปัตยกรรมระบบเครือข่าย ได้แก่ ๖.๑ แยกเครือข่ายสำรองข้อมูลออกจากเครือข่ายหลักและจำกัดสิทธิการเข้าถึงเครือข่ายสำรอง ๖.๒ สำรองข้อมูลตามรายละเอียด ดังนี้ ๑) กำหนดตารางการสำรองข้อมูลส่วนเพิ่ม (Incremental Backup) ในทุกวัน ตั้งแต่วันจันทร์ถึงวันศุกร์ และสำรองข้อมูลทั้งระบบ (Full Backup) ในทุกวันศุกร์ ๒) จัดทำสำเนาการสำรองข้อมูลแบบ Offline Backup บนอุปกรณ์จัดเก็บข้อมูลภายนอกทุกวันจันทร์และวันพุธ	๑. การรักษาความปลอดภัยของระบบโครงสร้างพื้นฐาน (Critical Infrastructure Security) ๒. การรักษาความปลอดภัยระบบแอปพลิเคชั่น (Application Security) เช่น โปรแกรม Antivirus, Firewall หรือโปรแกรมการเข้ารหัส เป็นต้น ๓. การรักษาความปลอดภัยของระบบอินเทอร์เน็ต (Network Security) ๔. การรักษาความปลอดภัยให้กับข้อมูลที่เก็บในคลาวด์ (Cloud Security) ๕. การรักษาความปลอดภัยให้อุปกรณ์ Internet of Thing (Internet of Thing Security)

ความเสี่ยง	การควบคุมที่มีอยู่	กิจกรรมที่จะตรวจสอบ
๓. Cyber Security : การป้องกันระบบเทคโนโลยีสารสนเทศจากภัยคุกคามทางไซเบอร์ เนื่องจากเป็นเทคโนโลยีเก่าและมีอายุการใช้งานนานกว่า ๕ ปี รวมถึงภัยคุกคามที่มีการพัฒนาและปรับเปลี่ยนรูปแบบตลอดเวลา (ต่อ)	๓) แจ้งผู้พัฒนาระบบให้ทำการสำรองข้อมูลระบบงานทุกระบบเป็นประจำทุกสิ้นสัปดาห์ ๖.๓ ใช้ระบบอีเมลกลางของภาครัฐ (Mail go Thai) เพื่อป้องกันความสูญหายของข้อมูลที่รับส่งผ่านจดหมายอิเล็กทรอนิกส์ และเพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง ๖.๔ ใช้บริการพื้นที่คลาวด์ของภาครัฐ ทั้ง G-Cloud (GDCC) และ MOF Cloud เพื่อให้ระบบงานต่างๆ ของ สบน. มีความมั่นคงปลอดภัยอยู่ภายใต้มาตรฐานป้องกันเครือข่าย ที่ได้รับการยอมรับในระดับสากลที่มีความมั่นคงปลอดภัยสูง ๖.๕ จัดทำสื่อประชาสัมพันธ์ให้ความรู้ความเข้าใจในการใช้เทคโนโลยีให้ปลอดภัยผ่านอินทราเน็ต อีเมล และกลุ่มแชท สบน. (LINE) ๖.๖ มีการกำกับดูแลเตรียมความพร้อมรับมือภัยคุกคามทางไซเบอร์ (Cyber Resilience) โดยมีกรอบการดำเนินงานและแนวทางที่ใช้ในการกำกับดูแล และบริหารจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ในภาพรวมขององค์กร ที่สอดคล้องกับกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งเหมาะสมสอดคล้องกับขนาด และความซับซ้อนของการปฏิบัติงาน ๖.๗ มีการควบคุมและป้องกันความเสี่ยงของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของ สบน. เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย อุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูลและระบบงาน เป็นต้น รวมทั้งการตั้งค่าระบบงาน การเข้าถึงระบบงานและการจัดการสิทธิ์ การรักษาความมั่นคงปลอดภัยของข้อมูล การพัฒนาระบบงานที่มีความปลอดภัยตามขั้นตอนหรือกระบวนการในการพัฒนาระบบงาน (System Development Life Cycle : SDLC) การบริหารจัดการ patch โดยมีการใช้เทคโนโลยีอย่างเหมาะสม เพื่อให้ สบน. มีกระบวนการ เครื่องมือ และวิธีการในการควบคุมหรือลดผลกระทบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น	

ความเสี่ยง	การควบคุมที่มีอยู่	กิจกรรมที่จะตรวจสอบ
๓. Cyber Security : การป้องกันระบบเทคโนโลยีสารสนเทศจากภัยคุกคามทางไซเบอร์ เนื่องจากเป็นเทคโนโลยีเก่าและมีอายุการใช้งานนานกว่า ๕ ปี รวมถึงภัยคุกคามที่มีการพัฒนาและปรับเปลี่ยนรูปแบบตลอดเวลา (ต่อ)	๖.๘ บริหารจัดการช่องโหว่ทางด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถตรวจจับ วิเคราะห์ ติดตาม และแจ้งเตือนเหตุการณ์ผิดปกติหรือภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานหรือผู้รับผิดชอบรับทราบ และกำหนดแนวทางในการสื่อสารและการดำเนินการแก้ไขในเบื้องต้นได้อย่างทันการณ์	

ตัวอย่างกระดาษทำการการตรวจสอบ IT Security & Cyber Security
(IT General Control)

กระดาษทำการ IT ๖๕๐๑๑๔๐๑-๑

กระดาษทำการตรวจสอบหมายเลข :

เรื่องที่ตรวจสอบ : IT Security & Cyber Security (IT General Control)

ประเด็นการตรวจสอบ : การควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (General Control) มีประสิทธิภาพ ครอบคลุมการปฏิบัติงานด้านเทคโนโลยีสารสนเทศของ สบน.

วัตถุประสงค์ : เพื่อสอบทานการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (General Control)

ขอบเขตการตรวจสอบ : การสอบทานการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (General Control)

ผลการตรวจสอบ :

รายละเอียด	ผลการตรวจสอบ		
	มี	ไม่มี	เอกสารอ้างอิง
๑. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานบริหารหนี้สาธารณะ (สบน.)			
๑.๑ การทบทวนนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล สบน.			
๑.๒ การสำรองข้อมูลของระบบงาน			
๑.๓ การทดสอบระบบสารสนเทศ การทดสอบระบบสำรองข้อมูล การทดสอบการกู้คืนข้อมูล			
๑.๔ การบริหารจัดการคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นๆ			
๒. โครงสร้างทางด้านความมั่นคงปลอดภัยของของระบบสารสนเทศ			
๒.๑ การมอบหมาย,จำหน้าที่รู้รับผิดชอบด้านความมั่นคงปลอดภัย			
๒.๒ ความรู้ความสามารถพื้นฐานของเจ้าหน้าที่รู้รับผิดชอบด้านความมั่นคงปลอดภัย เพียงพอ ,เหมาะสมต่อการปฏิบัติงาน			
๒.๓ การบริหารจัดการความมั่นคงปลอดภัย เช่น ระบบงานเกิดปัญหาขัดข้องไม่สามารถดำเนินการได้อย่างต่อเนื่อง เป็นต้น			
๓. การควบคุมการเข้าถึง			
๓.๑ การกำหนดรหัสผ่านเข้าเครื่องคอมพิวเตอร์			
๓.๒ มีการกำหนดสิทธิ์ผู้ดูแลระบบ ผู้ใช้งานระบบและการบริหารรหัสผ่าน มีตารางแสดงสิทธิการเข้าถึงฐานข้อมูล มีการควบคุม และจำกัดสิทธิ (ไฟล์เอกสารการกำหนดสิทธิ : ตารางกำหนดสิทธิ) รวมทั้งมีการทบทวนสิทธิเข้าถึงของผู้ใช้งานอย่างต่อเนื่องเป็นระยะตามที่กำหนดไว้ รวมทั้งมีการกำหนดรหัสผ่านสำหรับการเข้าถึงข้อมูลที่สำคัญ			
๔. ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อมของหน่วยงาน			
๔.๑ มีการบริหารจัดการรักษาความปลอดภัยทางกายภาพ (Physical Security Management)			

/รายละเอียด ...

รายละเอียด	ผลการตรวจสอบ		
	มี	ไม่มี	เอกสารอ้างอิง
และควบคุมพื้นที่การเข้า - ออกพื้นที่ควบคุม ได้แก่ ห้องปฏิบัติการคอมพิวเตอร์			
๕. ความปลอดภัยในการปฏิบัติงาน			
๕.๑ การติดตั้งระบบรักษาความปลอดภัย (เช่นการตรวจจับการแจ้งเตือนการบุกรุก, โปรแกรมสแกนไวรัสคอมพิวเตอร์ เป็นต้น)			
๕.๒ การบันทึก log			
๖. การควบคุมการพัฒนาและการบำรุงรักษาระบบสารสนเทศ			
๖.๑ มีการวางแผนการพัฒนาระบบ			

กระดาษทำการ IT ๖๕๐๑๑๔๐๒-๑

กระดาษทำการตรวจสอบหมายเลข :

เรื่องที่ตรวจสอบ : IT Security & Cyber Security (IT General Control)

ประเด็นการตรวจสอบ : การดำเนินการตามระบบ IT Security

วัตถุประสงค์ : เพื่อสอบทานการดำเนินการตามระบบ IT Security ว่า มีความเหมาะสม เพียงพอ

ขอบเขตการตรวจสอบ : การสอบทานการดำเนินการตามระบบ IT Security

ผลการตรวจสอบ :

รายละเอียด	ผลการตรวจสอบ		
	มี	ไม่มี	เอกสารอ้างอิง
๑. การรักษาความปลอดภัยเครือข่าย (Network Security)			
๑.๑ การกำหนดหน้าที่ความรับผิดชอบ			
๑.๒ การเชื่อมต่อเครือข่าย			
๑.๓ มีการกำหนดชั้นความลับของข้อมูล			
๑.๔ การดูแลเส้นทางของอุปกรณ์เครือข่าย			
๑.๕ การเชื่อมต่อเครือข่าย			
๑.๖ การตรวจจับและการป้องกันการบุกรุก			
๑.๗ แผนผังระบบเครือข่าย			
๑.๘ การบันทึกการทำงานของระบบป้องกันการบุกรุก			
๒. การรักษาความปลอดภัยอินเทอร์เน็ต (Internet Security)			
๒.๑ การเข้าสู่ระบบเครือข่ายภายใน สบน.			
๒.๒ การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (log) ของอุปกรณ์เครือข่าย			
๓. การรักษาความปลอดภัยอุปกรณ์ปลายทาง (Endpoint Security			
๓.๑ การยืนยันตัวตนในการเข้าใช้งานระบบสารสนเทศ			
๓.๒ การจัดการกับมัลแวร์หรือการโจมตีของไวรัส			
๔. การรักษาความปลอดภัยระบบคลาวด์ (Cloud Security)			
๔. การรักษาความปลอดภัยระบบคลาวด์ (Cloud Security)			
๕. การรักษาความปลอดภัยการเข้าใช้งานแอปพลิเคชั่น (Application Security)			
๕.๑ การใช้งานแอปพลิเคชั่น			
๕.๒ Application Security			